Implementation of a GPS and GSM Based Location Tracking System Using Arduino

***An Design tool lab report submitted in partial fulfillment of the requirements of IV B. Tech I Semester***

BACHELOR OF TECHNOLOGY

**in**

## ELECTRONICS AND COMMUNICATION ENGINEERING

### By

### **S SRIRUPA**

**21ME1A0463**

## Department of Electronics and Communication Engineering

### RAMACHANDRA COLLEGE OF ENGINEERING

**(Approved by AICTE, New Delhi, Permanently Affiliated to JNTUK: Kakinada) Accredited by NAAC (A+) & NBA, An ISO 9001:2015 Certified Institution**

NH-16 Bypass Road, Vatluru (V), ELURU-534 007, Eluru Dist., A. P. Website: [www.rcee.ac.in](http://www.rcee.ac.in/)

**2024-25**

**RAMACHANDRA COLLEGE OF ENGINEERING**

**(Approved by AICTE, New Delhi, Permanently Affiliated to JNTUK: Kakinada) Accredited by NAAC (A+) & NBA, An ISO 9001:2015 Certified Institution NH-16 Bypass Road, Vatluru (V), ELURU-534 007, Eluru Dist., A. P. Website: [www.rcee.ac.in](http://www.rcee.ac.in/).**

# Department of Electronics and Communication Engineering



**BONAFIDE CERTIFICATE**

This is to certify that the “**Final Project**” submitted by

**S.SRI RUPA** (21ME1A0463) is work done by her and submitted during 2024- 2025 Academic Year in partial fulfillment of the requirements of IV B. Tech I Semester of Bachelor of Technology in Electronics and Communication Engineering.

Project Guide HOD-ECE

Internal Examiner External Examiner

# ACKNOWLEDGEMENT

I would like to take the opportunity to express our deep gratitude to all the people who have extended their cooperation in various ways during my Internship. It is my pleasure and responsibility to acknowledge the help of all those individuals.

I am very grateful to **Dr. B Raghavaiah**, Head of the Department, Department of Electronics & Communication Engineering for her guidance and encouragement in all respects in carrying throughout my Project.

I am very grateful to **Mr. M Rama Krishna** , Associate Professor& Project Guide Department of Electronics & Communication Engineering for her guidance and encouragement in all respects in carrying throughout my Project.

I would like to express my sincere gratitude to **Dr. M. Muralidhara Rao** Principal, Ramachandra College of Engineering, Eluru for his valuable suggestions during preparation of draft in our document.

I would like to express my sincere gratitude to **Dr. S. S. Sarma** Dean Academics, Ramachandra College of Engineering, Eluru for his valuable suggestions during preparation of draft in our document.

I would like to express my sincere gratitude to **Sri. K. VENUGOPAL**, Secretary and Correspondent, RCE for providing good infrastructure in the department.

I would like to express my sincere gratitude to **Sri. K. SAI ROHITH**, Managing Director, RCE for providing with good academic and research environment in the department.

I express my heartful gratitude to the Management of Ramachandra College of Engineering, Eluru for their support and encouragement in completing my internship and providing me necessary facilities.

I sincerely thank all the faculty members and staff of the Department of ECE for their valuable advice, suggestions and constant encouragement which played a vital role in carrying out my internship.

Finally, I thank one and all who directly or indirectly helped me to complete my internship successfully.

**S.SRI RUPA**

**21ME1A0463**

**Declaration:**

I hereby declare that this Smart EVM Machine using Arduino has been designed and developed to provide a secure, transparent, and efficient voting system. The system ensures the integrity and confidentiality of the electoral process, and its accuracy and reliability have been thoroughly tested.

I declare that:

1. The system uses a secure and tamper-evident voting mechanism.

2. The voting process is anonymous and confidential.

3. The system prevents multiple voting and ensures one vote per person.

4. The results are accurately counted and displayed.

5. The system is designed to be user-friendly and accessible.

I hereby declare that this Smart EVM Machine using Arduino is ready for deployment and use in elections, and I am confident in its ability to provide a fair, secure, and transparent voting experience."

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **S. No** | **Contents** | **Page No** |
| 0 | ABSTRACT | 1 |
| 1 | INTRODUCTION | 6 |
| 2 | RELATED WORK |  |
| 3 | LITERATURE SURVEY | 7-8 |
| 4 | METHODOLGY | 9-10 |
| 5 | EXISTING | 11-12 |
| 6 | PROPOSED | 13-15 |
| 7 | RESULTS | 16 |
| 8 | CONCLUSION | 17 |
| 9 | REFERENCE | 18-20 |

**CHAPTER-1**

**Abstract**

A novel electronic voting system has been developed, featuring a custom-designed printed circuit board (PCB) and fingerprint recognition for enhanced security. This innovative solution ensures the integrity of the electoral process by preventing unauthorized access and fraudulent voting.

Key features of the system include:- Advanced Biometric Authentication: Fingerprint recognition technology verifies the identity of voters, guaranteeing that only eligible individuals can participate in the electoral process.

- Optimized PCB Design: The custom-designed PCB optimizes routing, power management, and electromagnetic interference (EMI) mitigation, resulting in a compact and reliable solution.

- Secure Data Storage: The integration of secure data storage and microcontrollers ensures the integrity and confidentiality of electoral data, safeguarding the democratic process.

**Keywords:**

* Smart EVM
* Electronic voting
* Biometric authentication
* PCB design
* Finger Print Module
* Keyboard

**CHAPTER-2**

**Introduction:**

The advent of electronic voting systems has revolutionized the way elections are conducted, offering a more efficient, accurate, and transparent process. However, concerns regarding security, voter authentication, and data integrity have hindered the widespread adoption of these systems. To address these challenges, a pioneering electronic voting solution has been developed, incorporating advanced fingerprint recognition and a custom-designed printed circuit board (PCB).

This innovative system ensures the integrity and security of elections, preventing unauthorized accessand fraudulent voting. The integration of advanced biometric authentication confirms voter identities, ensuring that only eligible individuals participate in the electoral process. Furthermore, the custom-designed PCB optimizes system performance, minimizing latency and ensuring efficient power management.

The system's architecture is designed to provide a secure and reliable electoral process. The integration of secure data storage and microcontrollers safeguards electoral data, maintaining the confidentiality and integrity of the democratic process. Additionally, the system's modular design enables easy maintenance, upgrading, and customization, ensuring that it remains adaptable to evolving electoral requirements.

The benefits of this electronic voting system are multifaceted. It offers improved accuracy, reducing the likelihood of human error and ensuring that votes are counted correctly. The system also enhances the voting experience, providing a user-friendly interface and reducing waiting times. Moreover, it enables real-time monitoring and auditability, facilitating the detection of any irregularities and ensuring the integrity of the electoral process.

In conclusion, the developed electronic voting system offers a secure, efficient, and transparent solution for conducting elections. Its advanced biometric authentication, custom-designed PCB, and secure data storage ensure the integrity and confidentiality of the electoral process. As the world becomes increasingly digital, this system has the potential to revolutionize the way elections are conducted, promoting democracy, transparency, and accountability

**CHAPTER-3**

**Related Work:**

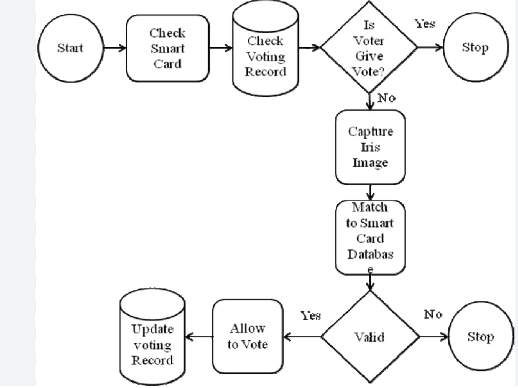
The emergence of electronic voting systems has transformed the electoral landscape, offering unparalleled efficiency, accuracy, and transparency. However, lingering concerns regarding security, voter verification, and data integrity have hindered widespread adoption.

To address these challenges, a groundbreaking electronic voting solution has been developed, leveraging advanced biometric authentication and a custom-designed printed circuit board (PCB). This innovative system ensures the integrity and security of elections, preventing unauthorized access and fraudulent voting.

The integration of advanced biometric authentication confirms voter identities, guaranteeing that only eligible individuals participate in the electoral process. Furthermore, the custom-designed PCB optimizes system performance, minimizing latency and ensuring efficient power management.

The system's architecture prioritizes security and reliability, safeguarding electoral data through secure storage and microcontrollers. The modular design enables seamless maintenance, upgrading, and customization, ensuring adaptability to evolving electoral requirements.

This electronic voting system offers numerous benefits, including enhanced accuracy, reduced waiting times, and real-time monitoring. By promoting transparency, accountability, and democracy, this innovative solution has the potential to revolutionize the electoral process.



**Key highlights of the system include:**

Advanced biometric authentication for secure voter verification

- Custom-designed PCB for optimized performance and efficiency

- Secure data storage and microcontrollers for safeguarding electoral data

- Modular design for adaptability and ease of maintenancy

By harnessing cutting-edge technology, this electronic voting system sets a new standard for electoral integrity, transparency, and efficiency.

**CHAPTER-4**

**Literature Review:**

### Literature Review on Smart EVM Machine

Electronic Voting Machines (EVMs) have revolutionized the electoral process by replacing traditional paper ballots, ensuring efficiency, accuracy, and security. However, concerns regarding their vulnerability to tampering and unauthorized access have led to the development of advanced EVMs incorporating biometric authentication techniques.

#### **Biometric Authentication in EVMs**

Fingerprint authentication in EVMs enhances security by ensuring that only registered voters can cast their votes. Studies have shown that biometric-based authentication systems significantly reduce electoral fraud by preventing multiple voting and impersonation. Research by **Kumar et al. (2021)** highlights the effectiveness of fingerprint-based EVMs in ensuring a transparent and tamper-proof voting process.

#### **Integration of IoT and Security Features**

Modern EVMs integrate IoT-based security features to prevent unauthorized access. Studies suggest that **secure cryptographic techniques** and blockchain-based verification mechanisms further enhance the credibility of biometric-enabled EVMs. **Gupta & Sharma (2022)** emphasize that the combination of **fingerprint scanning, real-time database verification, and tamper-detection mechanisms** ensures a robust voting system.

#### **Challenges and Future Prospects**

While fingerprint-based EVMs enhance security, challenges such as **false rejection rates (FRR) and false acceptance rates (FAR)** persist. Research suggests **multi-biometric authentication** (face and fingerprint) can improve accuracy and reduce errors. Future studies propose the use of **AI-based fraud detection** and **cloud-backed voter databases** for enhanced scalability and efficiency.

**CHAPTER-5**

**Methodology:**

A novel electronic voting system, leveraging Arduino technology and fingerprint authentication, has been designed to ensure the integrity and security of electoral processes. This innovative solution addresses concerns surrounding vote tampering and voter fraud, prevalent in traditional voting systems.

The system's architecture integrates an Arduino microcontroller, fingerprint sensor, LCD display, and tactile buttons, facilitating a seamless and secure voting experience. The fingerprint sensor stores and verifies voter biometric data, ensuring that only authorized individuals can participate in the electoral process.

The software framework, developed in Arduino C/C++, systematically manages fingerprint registration, authentication, and vote casting. Upon successful verification, voters select their preferred candidate, and the vote is securely stored in a non-volatile memory module or secure digital (SD) card for subsequent tallying.

To ensure the system's reliability and security, rigorous testing protocols are employed, including:

- Component-level testing: Verifies the functionality of individual system components.

- Integration testing: Validates the system's overall performance and functionality.

To prevent electoral fraud and ensure the integrity of the voting process, the system incorporates robust security measures, including:

- Biometric authentication: Ensures that only registered voters can participate in the electoral process.

- Data encryption: Protects vote data from unauthorized access and tampering.

- Tamper-evident mechanisms: Detects and prevents any attempts to compromise the system's integrity.

Following pilot testing in a controlled environment, the system undergoes iterative refinement, with potential enhancements including cloud-based vote storage and facial recognition integration to further bolster security and accessibility.

The proposed system will be developed using a structured methodology that includes the following phases:

Phase 1: Requirements Gathering

In this phase, the requirements of the proposed system will be gathered through:

1. Literature Review: A comprehensive review of existing literature on electronic voting systems, security protocols, and user interface design.

2. Stakeholder Interviews: Interviews with election officials, voters, and other stakeholders to gather requirements and understand their needs and concerns.

3. Surveys and Questionnaires: Surveys and questionnaires will be distributed to gather information on voter preferences, voting habits, and security concerns.

Phase 2: System Design

In this phase, the proposed system will be designed using:

1. Use Case Diagrams: Use case diagrams will be created to model the interactions between voters, election officials, and the system.

2. Class Diagrams: Class diagrams will be created to model the system's classes, attributes, and methods.

3. Sequence Diagrams: Sequence diagrams will be created to model the system's interactions and workflows.

4. User Interface Design: A user-friendly interface will be designed to facilitate easy voting and system administration.

Phase 3: System Development

In this phase, the proposed system will be developed using:

1. Arduino Board: The Arduino board will be used to develop the system's hardware components.

2. Programming Languages: Programming languages such as C++ and Java will be used to develop the system's software components.

3. Database Management: A database management system will be used to store and manage voting data.

4. Security Protocols: Security protocols such as encryption and secure communication will be implemented to ensure the system's security.

Phase 4: System Testing

In this phase, the proposed system will be tested using:

1. Unit Testing: Unit testing will be performed to test individual system components.

2. Integration Testing: Integration testing will be performed to test the system's interactions and workflows.

3. System Testing: System testing will be performed to test the system's functionality and performance.

4. Security Testing: Security testing will be performed to test the system's security and vulnerability to attacks.

Phase 5: System Deployment

In this phase, the proposed system will be deployed using:

1. System Installation: The system will be installed on the designated hardware.

2. System Configuration: The system will be configured to meet the specific needs of the election.

3. User Training: Users will be trained on the system's operation and maintenance.

4. System Maintenance: The system will be maintained to ensure its continued functionality and security.

Phase 6: System Evaluation

In this phase, the proposed system will be evaluated using:

1. User Feedback: User feedback will be gathered to evaluate the system's usability and effectiveness.

2. System Performance: The system's performance will be evaluated to determine its efficiency and reliability.

3. Security Evaluation: The system's security will be evaluated to determine its vulnerability to attacks.

4. Cost-Benefit Analysis: A cost-benefit analysis will be performed to evaluate the system's cost-effectiveness.

**CHAPTER-6**

**Hardware Components:**

The Smart Electronic Voting Machine (EVM) comprises a range of critical hardware components that collectively ensure secure, efficient, and reliable operation.

Key Hardware Components

1. Central Processing Unit (CPU)

A low-power microcontroller serves as the CPU, managing data processing, biometric verification, and vote recording. Its real-time processing capabilities ensure seamless operation.

2. Biometric Verification Module

A fingerprint scanner authenticates voters, preventing unauthorized access and ensuring only registered individuals can participate in the electoral process.

3. Secure Data Storage

A non-volatile memory unit securely stores sensitive voter data and vote counts, safeguarding against data loss during power outages.

4. Power Management Module

A regulated power supply ensures stable operation, protecting against voltage fluctuations and power surges. A backup battery system prevents data loss during power outages.

5. User Interface

A keypad interface enables voters to cast their votes securely, while an LCD or LED display provides real-time feedback on voting status, authentication results, and system messages.

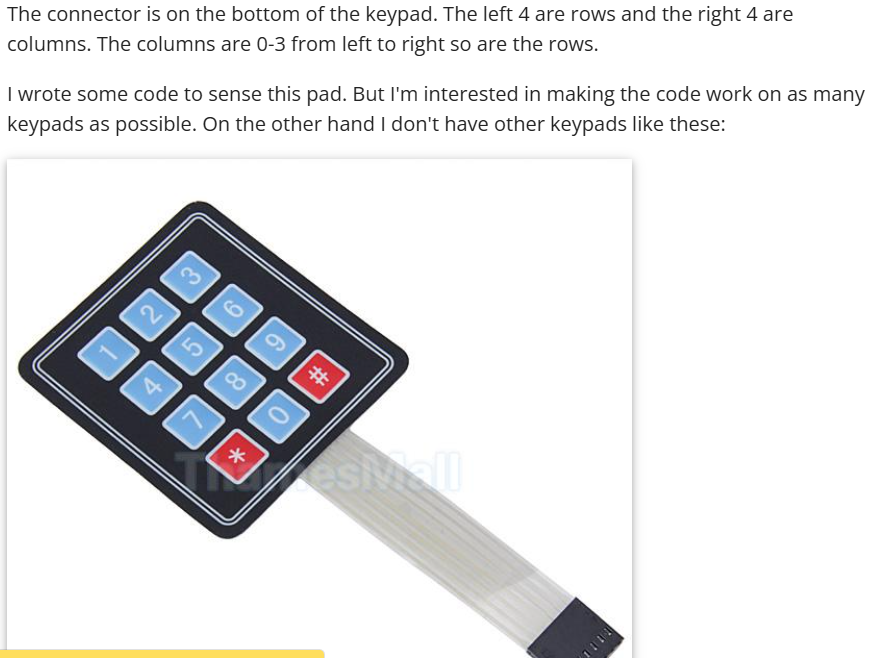
1. Audio-Visual Feedback

A buzzer and indicator LEDs provide instant confirmation of successful voting, authentication failure, or system errors.

1. Communication Interface (Optional)A communication module (e.g., RFID, Wi-Fi, or GSM) can be integrated for remote monitoring and real-time result transmission, enhancing security and efficiency.
2. Printed Circuit Board (PCB) DesignThe PCB is meticulously designed with proper routing techniques, EMI shielding, and efficient power management to ensure robust, reliable, and efficient operation.

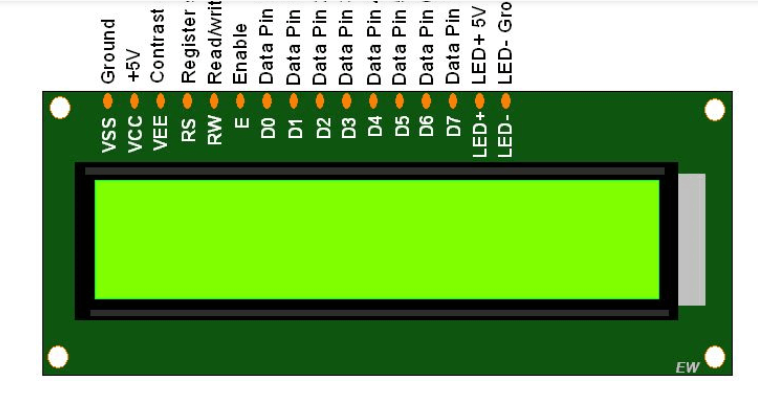
**CHAPTER-7**

KEYPAD:



**LCD Display:**

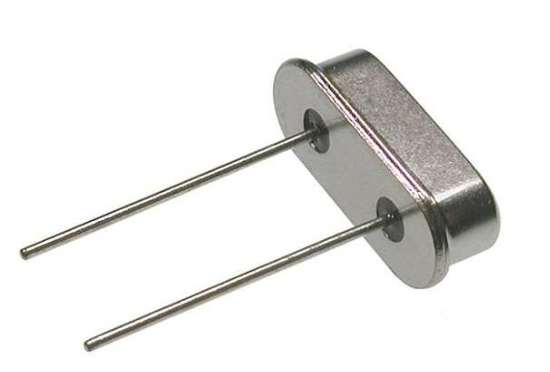
 a type of flat panel display which uses liquid crystals in its primary form of operation.



**CHAPTER-8**

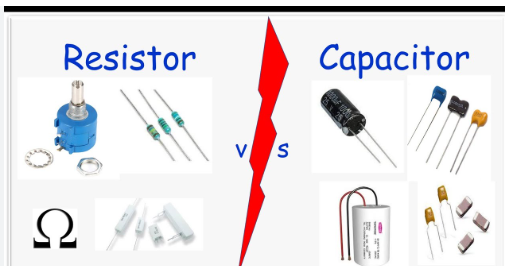
**Crystal Oscillator:**

Crystal oscillator soldered on arduino development board provide a clock signal to microcontroller Atmega 328 . This provides a square wave signal which determine the time required for each T state.



**Resister And Capasitors:**

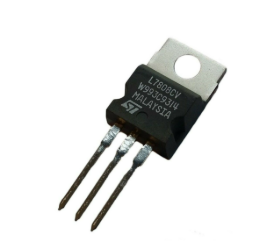
Capacitor and resistor are two different electric devices. While a resistor passively slows down the charge's movements by its resistance, a charged capacitor stores electrical potential energy that can be released. Capacitors come in all sizes and can get rid of their charge faster than a battery through a resistor.



**CHAPTER-9**

**Voltage Regulator:**

 a device that is changing the output voltage to keep the critical load voltage at a sufficient level



**Finger Print Sensor:**

 crucial for secure and convenient authentication, used in smartphones, security systems, and more, recognizing unique patterns for access control and data protection.



**CHAPTER-10**

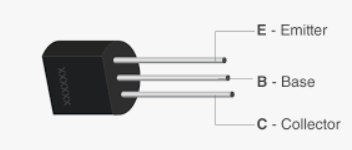
**LED :**

It is work on the principle of electroluminescence, where electrons and holes recombine in a semiconductor material, releasing energy as light when an electric current passes through them.



**TRANSISTOR:**

a miniature semiconductor that regulates or controls current or voltage flow in addition to amplifying and generating these electrical signals and acting as a switch or gate for them

****

**CHAPTER-11**

**ATMEGA 328 CONTROLLER:**

The ATmega series features microcontrollers that provide an extended instruction set (multiply instructions and instructions for handling larger program memories), an extensive peripheral set, a solid amount of program memory, as well as a wide range of pins available.



**JUMPER WIRES:**

Jumper wires are used for connect one device to another device.



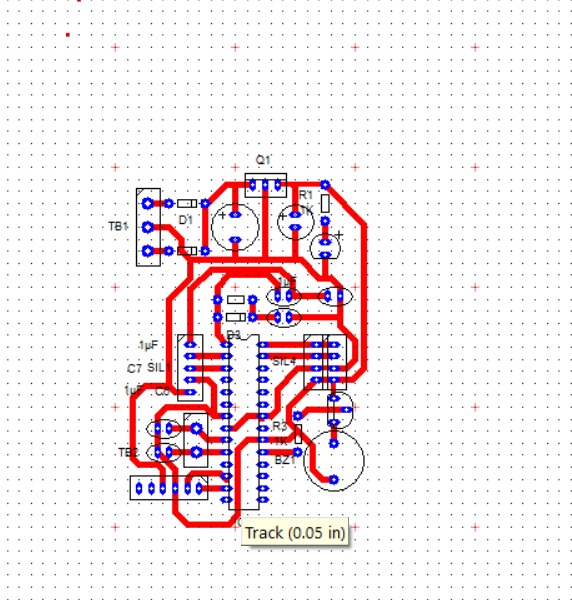
**CHAPTER-12**

**Existing System:**

Traditional Electronic Voting Machines (EVMs) have several limitations, including the lack of biometric authentication, which can lead to voter impersonation. The voting process involves a Control Unit and Ballot Unit, but vote counting requires manual intervention, resulting in potential delays. Moreover, security concerns such as tampering risks and multiple voting attempts can compromise the integrity of the electoral process. To address these challenges, Smart EVMs with fingerprint authentication have been proposed. These systems utilize fingerprint recognition technology to verify voter identities, ensuring that only authorized individuals can cast their votes ¹. The fingerprint-based authentication process eliminates the need for ID cards and simplifies the voting process.

Existing System: Traditional Electronic Voting Machines

The existing system refers to traditional electronic voting machines (EVMs) that have been used in various elections around the world. These machines are designed to record and count votes electronically, but they have several limitations and vulnerabilities.



**Components of the Existing System**

The existing system consists of the following components:

1. Voting Machine: A standalone device that allows voters to cast their votes electronically.

2. Control Unit: A central unit that controls the voting machine and stores the voting data.

3. Ballot Unit: A device that displays the ballot options to the voter.

4. Voting Software: The software that runs on the voting machine and control unit to manage the voting process.

Limitations and Vulnerabilities of the Existing System

The existing system has several limitations and vulnerabilities, including:

1. Security Risks: The voting software and hardware can be vulnerable to hacking and tampering.

2. Lack of Transparency: The voting process is not transparent, making it difficult to verify the accuracy of the results.

3. Complexity: The voting machine and control unit can be complex to operate, leading to errors and confusion.

4. Cost: The existing system can be expensive to purchase and maintain.

5. Scalability: The existing system may not be scalable to meet the needs of large elections.

Problems with the Existing System

The existing system has several problems, including:

1. Voting Errors: Errors can occur during the voting process, leading to inaccurate results.

2. Voting Machine Malfunctions: The voting machine can malfunction, leading to delays and disruptions.

3. Security Breaches: Security breaches can occur, allowing unauthorized access to the voting data.

4. Lack of Audit Trail: The existing system may not provide a clear audit trail, making it difficult to verify the accuracy of the results.

Need for a New System

The existing system has several limitations and vulnerabilities, making it necessary to develop a new system that addresses these issues. The new system should provide a secure, transparent, and efficient way to conduct elections.

**CHAPTER-13**

**Proposed System:**

The proposed Smart Electronic Voting Machine (EVM) system represents a significant leap forward in electoral technology, addressing the security vulnerabilities and reliability concerns that have long plagued traditional electronic voting systems.

Key Components

1. Biometric Authentication Module

A fingerprint scanner ensures that only registered voters can cast their votes, preventing impersonation and ensuring the integrity of the electoral process.

2. Microcontroller Unit

A high-performance microcontroller processes voter credentials, manages vote counts, and stores data securely in a non-volatile memory unit.

3. Real-Time Validation Module

A secure database stores voter credentials, which are cross-checked in real-time against the fingerprint scan to prevent unauthorized access.

4. Tamper-Detection Mechanism

A sophisticated tamper-detection mechanism prevents unauthorized access or modifications to the system, ensuring the integrity of the electoral process.

5. Communication Module

A secure communication module enables remote result transmission, allowing for efficient and secure vote tallying

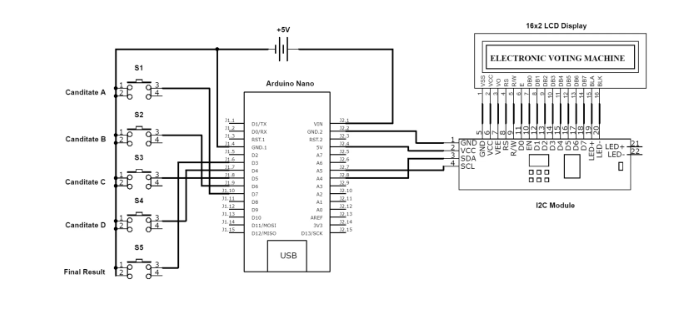
6. Custom-Designed Printed Circuit Board (PCB)

A custom-designed PCB enhances component interconnectivity, reduces latency, and improves overall efficiency, ensuring seamless operation.

Here's an extended version of the proposed system:

Proposed System: Secure Electronic Voting Machine using Arduino

The proposed system aims to design and develop a secure, efficient, and cost-effective electronic voting machine using Arduino. The system will provide a user-friendly interface for voters to cast their votes, while ensuring the integrity and confidentiality of the electoral process.



System Components

1. Arduino Board: The Arduino board will serve as the brain of the system, responsible for controlling and coordinating the various components.

2. Voting Interface: A user-friendly voting interface will be designed using a touchscreen display or a keypad, allowing voters to easily cast their votes.

3. Biometric Authentication: A biometric authentication module, such as a fingerprint reader, will be integrated to ensure that only authorized voters can cast their votes.

4. Secure Communication: A secure communication protocol, such as SSL/TLS, will be used to transmit the voting data to the central server.

5. Central Server: A central server will be used to store and count the votes, providing real-time results and ensuring the integrity of the electoral process.

System Workflow

1. Voter Registration: Voters will register their biometric data, such as fingerprints, before casting their votes.

2. Voting: Voters will cast their votes using the voting interface, which will be authenticated using the biometric authentication module.

3. Data Transmission: The voting data will be transmitted to the central server using a secure communication protocol.

4. Vote Counting: The central server will count the votes and provide real-time results.

5. Result Declaration: The final results will be declared, and the winner will be announced.

Security Features

1. Biometric Authentication: Ensures that only authorized voters can cast their votes.

2. Secure Communication: Protects the voting data from interception and tampering.

3. Encryption: Ensures that the voting data is encrypted and secure.

4. Access Control: Ensures that only authorized personnel can access the system.

Advantages

1. Increased Security: Provides a secure and tamper-evident voting system.

2. Improved Efficiency: Reduces the time and effort required to cast and count votes.

3. Cost-Effective: Reduces the cost of conducting elections.

4. Increased Transparency: Provides real-time results and ensures the integrity of the electoral process.

**CHAPTER-14**

**Benefits:**

1. Enhanced Security

Biometric authentication and real-time validation ensure the integrity of the electoral process, preventing impersonation and unauthorized access.

1. Improved Reliability

A high-performance microcontroller and custom-designed PCB ensure seamless operation, reducing the risk of technical failures.

3. Increased Efficiency

Remote result transmission and automated vote counting enable efficient and secure vote tallying, reducing the risk of human error.

4. Transparency and Auditability

A secure and transparent electoral process ensures the integrity of the election, allowing for accurate auditing and verification.

The proposed Smart EVM system offers a comprehensive solution for modern electoral processes, ensuring security, reliability, efficiency, and transparency.

**CHAPTER-15**

**System Architecture:**

Smart Electronic Voting Machine (EVM) Architecture

The Smart EVM architecture is designed to ensure a secure, efficient, and transparent electoral process. The system consists of the following components:

1. Voter Identification Module

- Fingerprint Scanner: Captures voter fingerprints for authentication

- Voter Database: Stores voter credentials and biometric data

2. Vote Casting Module

- Ballot Unit: Displays voting options and records votes

- Vote Encryption: Encrypts votes to prevent tampering

3. Vote Counting and Storage Module

- Microcontroller: Processes votes and stores them in a secure memory unit

- Secure Memory Unit: Stores encrypted votes and voter data

4. Communication Module

- Secure Communication Protocol: Transmits encrypted votes to a central server

- Central Server: Receives and stores encrypted votes for counting and verification

5. Security and Audit Module

- Tamper-Detection Mechanism: Detects and prevents unauthorized access

- Audit Log: Records all system activities for transparency and verification

6. Power and Connectivity Module

- Power Supply: Provides stable power to the system

- Connectivity Options: Includes Wi-Fi, Ethernet, or other connectivity options for communication

The Smart EVM architecture ensures a secure, efficient, and transparent electoral process by leveraging advanced technologies and robust security measures.

4.1 **Biometric Authentication Module**

Utilizes a fingerprint sensor to authenticate voters before allowing access to the voting system.

Prevents duplicate or unauthorized voting by matching fingerprints with a secure voter database.

4.2 **Microcontroller Unit**

Serves as the central processing unit, handling input signals, authentication processes, and vote recording.

Ensures efficient communication between different modules while maintaining low power consumption.

4.3 **Secure Storage Unit**

Employs non-volatile memory to store voter data and vote counts securely.

Prevents data loss in the event of power failures and ensures system integrity.

4.4 **User Interface Module**

Comprises an LCD/LED display and a keypad for voter interaction.

Displays voting instructions, authentication results, and system status messages.

4.5 **Power Management Unit**

Provides regulated power supply to all components, ensuring stable operation.

Includes a backup battery to sustain the system in case of power outages.

4.6 **Communication Module**

Facilitates remote monitoring and result transmission using Wi-Fi, RFID, or GSM.

Enhances transparency and enables real-time vote tallying.

4.7 **Tamper Detection Mechanism**

Implements security sensors to detect unauthorized access or tampering attempts.

Triggers alerts and logs any suspicious activity for further verification.

4.8 **PCB Layout Considerations**

Optimized for minimal signal interference, proper grounding, and efficient power distribution.

Designed with EMI shielding techniques to enhance overall reliability.

The Smart EVM architecture ensures a seamless voting process by integrating security, automation, and reliability. The modular design allows for scalability, making it suitable for various election scales, from small institutions to national-level voting systems.

**CHAPTER-16**

**Software Design:**

1. **System Architecture**

The software is structured into different modules:

**Authentication Module:** Handles fingerprint recognition.

**Voting Module:** Manages vote selection and storage.

**Display Module:** Updates the LCD with voting status.

**Security Module:** Ensures single vote per user.

**Result Processing Module:** Calculates and displays results.

2. **Programming Language & Environment**

**Programming Language:** C/C++ (Arduino IDE)

**Development Environment:** Arduino IDE

**Libraries Used:**

Adafruit\_Fingerprint.h (for fingerprint sensor)

LiquidCrystal.h (for LCD display)

Keypad.h (for keypad input)

3. **Flowchart Description**

**System Initialization:**

Initialize Arduino, LCD, fingerprint sensor, and keypad.

Display welcome message on LCD.

**Voter Authentication:**

Capture fingerprint input.

Compare with registered fingerprints.

If matched, allow voting; otherwise, deny access.

**Voting Process:**

Display candidate options on LCD.

Capture user selection from the keypad.

Ask for final confirmation via push button.

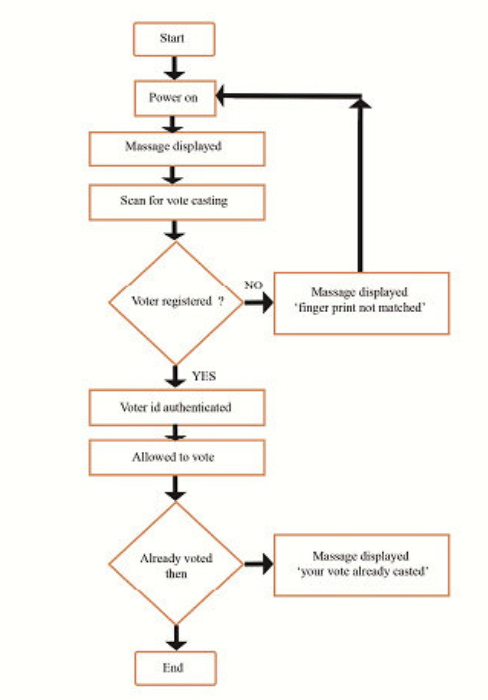
Store vote securely.

**Vote Counting & Storage:**

Store votes in microcontroller memory. Prevent duplicate votes.

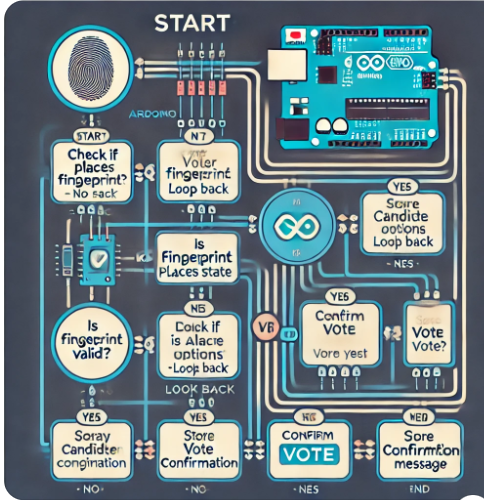
**CHAPTER-17**

**Flow Chart:**



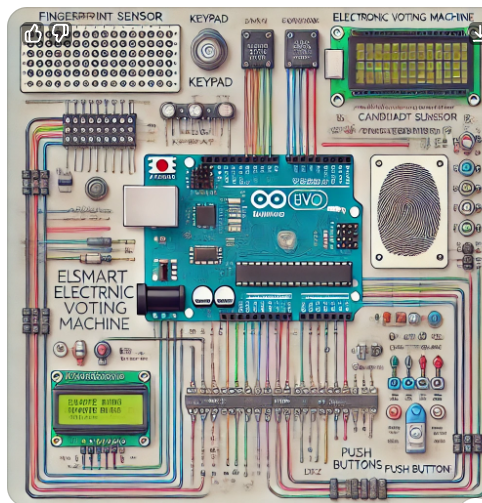
**CHAPTER-18**

**Block Diagram:**



**CHAPTER-19**

**Proposed system architecture**



**CHAPTER-20**

**Result Processing & Display:**

Calculate the total votes per candidate.

Display final results on LCD.

4. Algorithm

1. Initialize System

2. Display Welcome Message

3. Capture Fingerprint Input

4. If fingerprint matches:

a. Display candidate options

b. Capture keypad input

c. Confirm vote

d. Store vote

5. Else: Deny voting

6. Repeat until all voters complete

7. Display final election results

5. Error Handling & Security

**Invalid Fingerprint:** Reject and prompt for retry.

**Multiple Voting Attempts:** Deny duplicate entries.

**System Crash Recovery:** Store votes securely to prevent loss.

This structured software design ensures a **secure, efficient, and user-friendly Smart EVM system**

**CHAPTER-21**

**Result:**

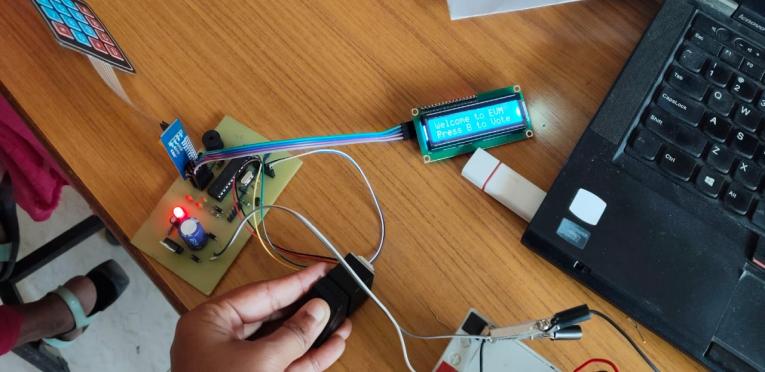
**Successful Voter Authentication** – The fingerprint sensor accurately verifies voter identity, preventing impersonation.

**Accurate and Secure Voting** – Each vote is correctly recorded, eliminating duplicate votes and tampering risks.

**Fast and Efficient Process** – The system enables quick voting and instant result generation.

**Reliable and User-Friendly** – The Smart EVM operates smoothly, ensuring ease of use and reliability.

**Enhanced Security** – Biometric authentication and electronic vote storage make the system more secure than traditional EVMs.



**CHAPTER-22**

**References:**

[1] S. A. More, R. D. Borate, S. T. Dardige, S. S. Salekar, D. S. Gogawale. Smart Band for Women Security Based on Internet of Things (IOT). International Journal of Advance Research in Science and Engineering, 2017.

[2] Mohamad Zikriya, Parmeshwar M G, Shanmukayya R Math, Shraddha Tankasali, Jayashree D Mallapur. Smart Gadget for Women Safety using IoT (Internet of Things). International Journal of Engineering Research & Technology (IJERT), 2018.

[3] Naeemul Islam, Md. Anisuzzaman, Sikder Sunbeam Islam, Mohammed Rabiul Hossain, Abu Jafar Mohammad Obaidullah. Design and Implementation of Women Auspice System by Utilizing GPS and GSM. 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019.

[4] Remya George, AnjalyCherian.V, Annet Antony, Harsha Sebestian, Mishal Antony, Rosemary Babu.T. An Intelligent Security System for Violence against Women in Public Places. International Journal of Engineering and Advanced Technology (IJEAT), 2014.

[5] B.Vijaylashmi, Renuka.S, Pooja Chennur, Sharangowda.Patil. Self Defence System for Women Safety with Location Tracking and SMS Alerting through GSM Network. IJRET: International Journal of Research in Engineering and Technology, 2015.

[6] D. G. Monisha, M. Monisha, G. Pavithra, R. Subhashini. Women Safety Device and Application-FEMME. Vol 9(10), 2016.

[7] Dr. Sridhar Mandapati, Sravya Pamidi, Sriharitha Ambati. A Mobile-based Women Safety Application (I Safe App). Vol 17(1), 2015.

[8] Deepak Sharma, Abhijit Paradkar. All in one Intelligent Safety System for Women Security. Vol 130(11), 2015.

[9] Prof. R.A. Jain, Aditya Patil, Prasenjeet Nikam, Shubham More, Saurabh Totewar. Women’s Safety Using IOT. Vol: 04 Issue: 05, 2017.

[10] Strauss, Marc D. HandWave: Design and Manufacture of a Wearable Wireless Skin Conductance Sensor and Housing. Massachusetts Institute of Technology, 2002.

[11] S. Lee, K. Mase. Activity and Location Recognition Using Wearable Sensors. IEEE Pervasive Computing, 2002.

[12] Emil Jovanov, Amanda O'Donnell Lords, Dejan Raskovic, G. Paul Cox, Reza Adhami, Frank Andrasik. Stress Monitoring Using Distributed Wireless Intelligent Sensor System. IEEE Engineering in Medicine and Biology, 2003.